Performance Work Statement (PWS)

National Ground Intelligence Center (NGIC) Combat Incident Database (CIDB) and Joint Trauma Analysis for the Prevention of Injury in Combat (JTAPIC) Database (JDB) (CJDB)

Short Title: NGIC CJDB
01/04/2017

Version 1.3

1. Government Points of Contract:

1.1 Contracting Officer Representative (COR)
The U.S. General Services Administration (GSA) Contracting Officer Representative (COR) for this task order is Carol Carpenter, 3QFAA, who can be reached at phone (301) 737-2493 ; e-mail: Carol.Carpenter@gsa.gov.

1.2 Technical Task Monitors.

a. Primary Technical Task Monitor (TTM).

Name:	Elisabeth Howe
Organization:	NGIC, ATTN: IANG-ITE-PM, MS106
DODAAC:	W26MT9 or HC1013-Army
Address:	2055 Boulders Road, Charlottesville, VA 22911-8318
Phone Number:	434-980-7590 DSN: 521-7590
Fax Number:	434-980-7407
E-Mail Address:	elisabeth.j.howe.civ@mail.mil

b. Alternate TTM.

Name:	Jeffry Boutet
Organization:	NGIC, ATTN: IANG-ITE-PM, MS106
DODAAC:	W26MT9 or HC1013-Army
Address:	2055 Boulders Road, Charlottesville, VA 22911-8318
Phone Number:	434-951-1794 DSN: 521-1794
Fax Number:	434-980-7407
E-Mail Address:	jeffry.c.boutet.civ@mail.mil

1.3 U.S. GENERAL SERVICES ADMINISTRATION (GSA) FEDERAL ACQUISITION SERVICE (FAS) TEAM - REGION 3

a. Contracting Officer (KO)

Name:	Angela Bennert
Organization:	GSA FAS AAS 3QZA
DODAAC:	473600
Address:	The DOW Bldg. - 3rd Flr. FAS AAS, 100 S. Independence Mall West, Philadelphia, PA 19106
Phone Number:	(215) 446-5818
E-Mail Address:	angela.bennert@gsa.gov

b. Contract Specialist (CS)

Name:	Ryan Mathews
Organization:	GSA FAS AAS 3QZA
DODAAC:	473600
Address:	The DOW Bldg. - 3rd Flr. FAS AAS, 100 S. Independence Mall West, Philadelphia, PA 19106
Phone Number:	(215) 446-5793
E-Mail Address:	ryan.mathews@gsa.gov

2. **Task Order (TO) Title**. National Ground Intelligence Center (NGIC) Combat Incident Database (CIDB) and Joint Trauma Analysis for the Prevention of Injury in Combat Database (JTAPIC) Database (JDB).

3. **Background**. NGIC created the CIDB in 2005 at the direction of the Army Staff. ALARACT 181/2008 levied the requirement that all available incident data be collected and stored within the CIDB.

- CIDB is built in Oracle and in compliance with the Department of Defense (DoD) standards
- The CIDB was approved by the G-2 to house both Personally Identifiable Information (PII) and Protected Health Information (PHI)
- The CIDB is intended to serve as the long term record of combat incidents for the Army

Based on these capabilities, the JTAPIC partners decided in FEB 2011 to use the CIDB as the basis for the JTAPIC Data Base application.

The system is comprised of two applications, which share a common database backend:

- Combat Incident Database (CIDB) application:
    - CIDB is an application used to store data in support of the NGIC Combat Incident Analysis Division (CIAD) mission to describe combat incidents with weapon, vehicle, and crew details; identify weapons used in an attack; identify most common and most dangerous (lethal) weapons; identify weapons effects on the system (vehicle damage and crew); and identify targeting trends and employment techniques to be incorporated into casualty analysis.
    - *Technical Specifications:*
        - Logical Source Lines of Code (LoC): 140,000
        - Technologies:
            - CIDB Front end: Apache, PHP, Tomcat 6, RedHat 6, Java
            - Back end: Pentaho, PL/SQL, Oracle 12c, Windows 2012
        - Customer Base: Army (both within NGIC and outside of NGIC), DoD, Intelligence Community (IC)
        - Networks: SIPRNet
        - External Interfaces: Yes
        - Certification Status: Certificate of Networthiness (CoN)
        - Current Development Location: On-site
- Joint Trauma Analysis for the Prevention of Injury in Combat (JTAPIC) Database (JDB)
    - The JDB provides a secure web-based portal accessing the common backend database that provides an environment to collect, integrate, analyze, and store information that individuals and groups can read, write, revise, and/or retrieve for the purpose of analyzing and disseminating actionable information to inform solutions that prevent or mitigate injury worldwide. The system accommodates data exchange with government agencies and affords protection and limited access to data that is personal identifiable information, protected health information, and intelligence/threat information.
    - *Technical Specifications:*
        - Logical Source Lines of Code (LoC): 25,000
        - Technologies:
            - JDB Front end: Apache, PHP, Tomcat 6, RedHat 6, Java
            - Back end: Pentaho, PL/SQL, Oracle 12c, Windows 2012
        - Customer Base: Army (both within NGIC and outside of NGIC), DoD, IC
          Networks: SIPRNet
        - External Interfaces: Yes

- Certification Status: CoN
- Current Development Location: On-site

The CIDB also supports an NGIC initiative for a project called Global aRchitecture for weApons, Incidents, and profiLes (GRAIL). GRAIL is not a separate application that must be supported, but is a project leveraging data from CIDB, System Parametric Information, Relational Intelligence Tool (SPIRIT), and potentially Biometric Identify Intelligence Resource (BI2R). This TO is specific to the requirements levied upon CIDB to support the GRAIL initiative; however, the CIDB team is expected to coordinate with the SPIRIT team, at the informal working level, to implement mutually supporting requirements as defined in PWS section 6.4.4.

The operational level maintenance for the NGIC IT infrastructure is performed by NGIC IT services personnel and is not part of the CJDB Task Order (TO) requirement. This includes Oracle database patches, RedHat Linux upgrades, Java upgrades, etc. CJDB personnel under this TO are required to ensure the CIDB and JDB continue to function as these updates are deployed (PWS 6.4.3).

The CIDB and JDB are currently developed using a modified Waterfall development methodology, but this methodology is not mandated or required. Historically, the government has received three software releases per year (combination of major and minor), with 1-3 emergency release patches.

4. **Objective**. The Contractor is responsible for enhancing the CIDB and JDB based on the requirements identified in task 6.4, evolving the design to a Model-View-Controller (MVC) pattern, evolving the development methodology using a more iterative approach, and for maintaining system certification and accreditation for the CIDB and JDB.

5. **Scope**. The scope of this TO is to support the continued operation and maintenance of the CIDB and JDB. It supports the NGIC and JTAPIC, along with several other stakeholders in providing detailed intelligence information regarding the record of combat incidents. This TO includes the following tasks:

- Task 1 – Technical Project Management
- Task 2 – Application Administration
- Task 3 – Data Administration
- Task 4 – Operations and Maintenance
- Task 5 – Requirements Management
- Task 6 – Information Assurance

6. Performance Requirements

6.1 Technical Project Management – Task 1.

The Contractor shall provide Technical Project Management In Accordance With (IAW) NGIC IT standards and industry best practices such as those in DOD-STD-2167 and ISO/IEC/IEEE 26515:2011 for iterative development methodologies. The Contractor shall provide the activities needed for the management of this PWS including management of TO employees, quality assurance, progress/status reporting, schedule development, risk identification/handling/mitigation strategy, and program reviews. The Contractor shall participate in required weekly TTM meetings and quarterly/IPR status reviews. The Contractor shall document and maintain software development team coding standards, development processes, and cross-training of team members in software development functional areas across technologies.

6.1.1 Task Order Management Plan (TOMP). The Contractor shall create, maintain, and deliver a TOMP IAW the following elements at a minimum:

1. Background - Summary of the Contractor's approach to meet task requirements
2. Roles - Identify resources that will be performing on the TO and their responsibilities
3. Communication - Identify how the Contractor will meet the reporting requirements identified in the TO
4. Risk - Outline the approach for managing risks encountered during the performance on the TO
5. Contract Work Breakdown Structure (CWBS) – which represents the Contractor's plan to accomplish the entire task order. The CWBS shall serve as the framework for the task schedule, budgeting, and reporting of technical, cost and schedule status to the COR & TTM. The CWBS shall provide a structured approach to the accomplishment of requirements of the CIDB/JDB systems by defining, allocating, and resourcing work to the appropriate CWBS element. The Contractor shall closely monitor execution of tasks against the allocated CWBS element and resources consumed. This should clearly define the team roles and delineate staffing for development, application administration, and data administration.

6.1.2 Integrated Master Schedule (IMS). The Contractor shall provide and maintain an Integrated Master Schedule (IMS) detailing when the Contractor plans to accomplish the entire TO's work scope. The IMS is comprised of the milestones and requisite activities for all work performed under the task order, to include required meetings, deliverables, and dependencies. The contractor may propose changes to the IMS to enhance effectiveness in satisfying program objectives. Any changes to the schedule shall be agreed upon by both the Contractor and Government at the weekly configuration change board (CCB) meetings. All known delays/impacts in scheduled deliverables shall be documented within the CCB meeting minutes detailing the affected deliverable task and a description of the cause. The Contractor may propose changes to the IMS to enhance effectiveness in satisfying program objectives. These changes can be raised at the Weekly IPT to the TTM and functionality representative, who will approve or disapprove the change in writing. The Contractor shall present this project status information in an Adobe PDF or compatible electronic format at every CCB.

6.1.3 Monthly Status Report (MSR). The Contractor shall provide a written Monthly Status Report (MSR) to the TTM and COR. The MSRs shall detail: work accomplished during the calendar reporting period, including risk, schedule, and technical status; work planned to be accomplished in the subsequent calendar reporting period, and expenditures to date. MSRs shall be synchronized with the monthly invoice. The COR & TTM will provide technical guidance for necessary changes in the content or format of the report as necessary during the period of performance to ensure the Government receives required information in the MSRs. The Government will have 10 days to accept or reject with comments and the MSR shall be submitted to the Government COR & TTM No Later Than (NLT) the tenth business day of the subsequent month.

The Contractor shall present this task status information in an electronic format or other format as approved by the Government. The MSR shall relate technical accomplishment to schedule status and contain the following elements:

1. Agency Name - identify the name of the agency sponsoring the task.
2. Task Name - identify the name of task, contract number (including TO number) and contract history.
3. Review Period -indicate the review period covered by this report.
4. Date - identify the date of the report and the date of the data contained within the report.

5. Contact Information - identify the name and phone number of the individual to contact for follow-up information on the report.
6. Schedule Status -
   - a. Include a high-level schedule that shows the key milestones of the task, from task order start through completion.
   - b. Current Period - list the key planned and actual start/completion dates for milestones and events for the current month by IMS. Identify dependencies on external resources (e.g., test server must be available for use by [date]). Explain the reasons for variance and planned corrective actions.
   - c. Upcoming Report Period - List key planned milestones and activities for the upcoming report period by IMS. Identify dependencies on external resources (e.g., test server must be available for use by [date]).
   - d. All milestones and deliverable dates shall be traceable to the task schedule.
7. Technical/Performance Status -
   - a. Include key technical performance measures (number of new change requests and number of outstanding defects).
8. Task Risks - describe any risks that need to be communicated to or addressed by the Government, the impact to TO performance, and the mitigation the Contractor has in place (see PWS Section 6.1.5 Risk Management).
9. Task Issues - describe any major issues that need to be communicated to or addressed by the Government.
10. Task Quality Activities - describe activities related to quality assurance, quality improvement or performance measurement including results of process audits and code walkthroughs.
11. Action Items - Status of both Contractor and Government action items which impact the task.

6.1.4 Communications. The Contractor shall communicate with the Government IAW the following guidelines.

1. Weekly Integrated Project Team Meeting (IPT)
   - a. The objective of the weekly status meeting is to:
     - i. Raise issues that need Government COR & TTM attention
     - ii. Review risks
     - iii. Review schedule
     - iv. Conduct release milestone reviews with stakeholders
     - v. Configuration Control Board (CCB)
       1. Review requirements being worked
       2. Review/approve/prioritize requirements for implementation (i.e., release planning)
       3. Create/review/update action items
   - b. The Contractor shall support the NGIC Functional Representative with creation of Weekly IPT meeting agenda, delivering it No Later Than (NLT) 2 business days prior to the Weekly IPT meeting.
   - c. The Contractor shall provide Meeting Minutes NLT 2 business days after the Weekly IPT
2. Quarterly In-Process Review (IPR)
   - a. The objective of the IPR is to address the following from the previous quarter:
     - i. Summarize technical scope of work (can be high-level CWBS)
     - ii. Current staffing status and alignment to tasks
     - iii. Identify key milestones that have been met, depicting any schedule deviations
     - iv. Identify key milestones upcoming for the remaining quarter(s)
     - v. Identify task level status, risks, issues, and mitigations

vi. Address high level requirements met during the preceding quarter's development sprints
vii. Address high level requirements planned to implement in the remaining quarter(s)

b. The Contractor shall provide an agenda for the IPR NLT 5 business days prior to the IPR
c. The Contractor shall provide the draft IPR slides to the Government COR & TTM NLT 5 business days prior to the IPR; final slides NLT 1 business day prior to the IPR.
d. The Contractor shall provide Meeting Minutes NLT 5 business days after the IPR

6.1.5 Risk Management. The Contractor shall develop and maintain a Risk Management Plan (RMP) detailing the approach for identifying, assessing, documenting, scheduling, resourcing, and tracking risks. For all risks identified, the Contractor shall analyze and prioritize each risk based on its potential impact and urgency. Additionally, the Contractor shall create a mitigation approach for each risk identified which will be communicated to the Government COR & TTM in the MSR.

The Contractor shall create a Risk Register, based on risks identified using the approach detailed in the RMP. The Risk Register will minimally include:

- Date Identified
- Title
- Description
- Impact – severity if risk is realized
- Probability – chance that the risk will occur
- Exposure – which is Impact x Probability
- Control / Mitigation plan
- Task Order Schedule milestone effected
- Risk Owner
- Status – Open / Closed

6.1.6 Quality Management. The Contractor shall prepare a Quality Management Plan (QMP) describing the Contractor's plans, procedures, metrics, and controls that will be used to substantiate product quality and fulfillment of TO requirements for each of the required software releases. The QMP shall include the Contractor's approach to gathering CIDB and JDB performance metrics baselines. The Contractor shall implement their approach to gathering CIDB and JDB performance metrics baselines through a Metrics Report.

The QMP identifies the means by which the Contractor will ensure quality assurance effectiveness and demonstrate comprehensive management and review of data, such that the results may be used to indicate trends and progress in quality of products as appropriate to this TO. The QMP describes what is measured, how often it is tracked, and who reviews and assures that appropriate action is initiated when trends are unfavorable. The QMP shall:

1. Identify how the Contractor will provide process-oriented Quality Assurance evaluations.
2. The set of operating procedures for planning, directing, monitoring and measuring work products. These procedures provide the controls for accurate decision-making data for the project management team to analyze and capture variances and plan revisions to the baseline costs.
3. Identify the processes and test criteria that will be used to demonstrate application performance.
4. Identify the approach for collection and reporting of performance metrics demonstrating progress.

The Metrics Report helps to ensure the CIDB and JDB are continually reviewed for acceptable application performance. The Metrics Report shall:

1. Include a matrix of the baseline performance of CIDB and JDB queries, exports, and customer reports.
2. The matrix shall include a table of system response times for Simple, Medium, and Complex queries (e.g., 1 filter, 3 filters, >3 filters) versus the number of results returned (0-50), 51-500, >500) for the CIDB and JDB Search, Flexible Search, and Custom Report features.
3. Be updated with each release to show that the system response performance is equal or improved.
4. With each release, include the number of software defects leaked into the Production system, with corresponding severity category.

6.1.7 Software Configuration Management. The Contractor shall establish and maintain a Software Configuration Management Plan (SCMP) based on the requirements for application configuration management in the current Defense Information Systems Agency (DISA) Application and Development STIG. Contractor will maintain software in a configuration management (CM) industry standard system (i.e.: GIT/Subversion) that will provide direct linkage from source code to the product backlog items (i.e.: Jira) that requested that item. The SCMP, at a minimum, defines the process and procedures the Contractor will use to track and control all software changes and documents the software baseline with proper revision control for all software and documentation configuration items.

The Contractor shall record and track software problems and change requests upon discovery, through Configuration Control Board approval, and ultimately to resolution.

6.1.8 Release Management. The Contractor shall deliver a Release Package with every software release to the NGIC networks. The Release Package shall contain the project schedule, System Requirements Specification (SRS), and the list of items included in the release (e.g., defects fixes, change requests, new requirements, etc.), release notes, source code, Entity Relationship Diagram (ERD), and DDL scripts, if applicable. The Release Package should be distinguishable for CIDB and JDB, such that a separate JDB Release Package could be distilled and delivered to the JTAPIC Program Management Office (PMO) without reference to CIDB-specific items. All included documentation shall be applicable to the current release. The release notes shall address the new functionality and refer to the requirement or bug fix that prompted the action. Prior to initiating activities on software releases, both the Government COR, TTM and functional representative must sign the Release Package. The second signatures of the Government COR, TTM and functional representative on the Release Package will document release acceptance in NGIC Pre-Production/UAT. The Contractor shall also follow procedures and documentation requirements outlined in the NGIC Software Development Life Cycle (SDLC) (Volume determined by release scope as Major, Minor, or Patch), and follow the NGIC Change Management process for creating and managing a Change Ticket in the Enterprise Service Center (ESC). Software deliveries shall be accompanied by updated Application User Manual/Guides, as application functionality is updated. The Application User Manual/Guide should be specific to the database they support (i.e., There shall be a distinct Application User Manual/Guide for the CIDB and another distinct Application User Manual/Guide for the JDB).

The recommended release cycle for software will be time-boxed to three to four months (e.g., two to three development sprints and one release sprint), in the NGIC test and pre-production environments, culminating to a minimum of three releases within a 12-month period. The requirements for reach release shall be determined and prioritized during the CCB, are generated from the process identified in PWS 6.5 (inclusive of PWS subsections), which meet the types of maintenance activities and high level requirements as identified in PWS 6.4 (inclusive of PWS Subsections).

Each development sprint is expected to contain 1-2 high-level features, (which equates to roughly 10-20 system level requirements per feature), as well as corrective, preventive, and adaptive maintenance activities. For each of the three releases (major or minor) the Contractor shall deliver a “shippable product,” release package, and is responsible for deploying to the NGIC test and pre-production environments, as well as on-site support to the government for the deployment of the release to the NGIC production environment.

Emergency releases (explained further in PWS 6.4.1) do not count towards the minimum required three releases per year; however, they must still be documented with a Release Package.

The following deliverables are applicable to PWS Section 6.1 and all of it’s subsections:

- Task Order Management Plan (TOMP)
- Integrated Master Schedule (IMS)
- Monthly Status Report (MSR)
- Weekly IPT Meeting
  - Agenda
  - Meeting Minutes
- Quarterly In-Process-Review (IPR) Briefing
  - Agenda
  - Presentation
  - Meeting Minutes
- Risk Management Plan (RMP)
- Risk Register
- Quality Management Plan (QMP)
- Metrics Report
- Software Configuration Management Plan (SCMP)
- Release Package(s)
- NGIC SDLC documentation commensurate with the scope of each release (Major, Minor, Patch, etc.)
- CIDB and JDB Application User Manual/Guide
- Documented Coding Standards and Development Processes

6.2 <u>Application Administration – Task 2</u>

The Contractor shall provide support to the production operation of CIDB and JDB by maintaining configuration settings across all NGIC environments to include:

- Configuration of role based access settings to include modifications to existing roles and creation of new roles
- Maintenance of default report formats in Pentaho
- Maintenance of Flexible search settings, adding and removing fields, and default search settings
- Administration of Strike Point drawings
- User account administration. The Contractor shall enable/disable accounts and assign users to roles per CIAD and JTAPIC User Account Standard Operating Procedures (SOPs)
- Configuration of Message of the Day notifications
- Documentation of daily metrics on system planned/unplanned availability, number of incident and person records, number of attached media, and a log of all known system changes (component upgrades, application releases)

The following deliverables are applicable to PWS Section 6.2:

- CIDB/JDB Account SOP
- Run Book

- Configuration Guide
- System Administration Guide
- Daily Application Metrics

6.3 Data Administration – Task 3

The Contractor shall administer digital content and support ad hoc query requests. The Contractor shall resolve data issues within CIDB and JDB. The Contractor shall manage and resolve inaccurate, duplicate, orphan, and incomplete data in coordination with the government subject matter expert. CIDB and JDB leverage third party systems such as Pentaho, WebTAS, and CIDNE, which support the import of incidents and incident data into CIDB and JDB. The Contractor shall ensure continued integration with these tools with each software release. The Contractor shall support data administration by maintaining pick list values and subsequently migrating legacy data to match new values. The Contractor shall also perform the following tasks to maintain data within the CIDB and JDB:

- Import of JTAPIC Injury data, maintenance of import template, and facilitation of error processing
- Import of JTAPIC Personal Protective Equipment (PPE) data, maintenance of import template, and facilitation of error processing
- Maintenance of JTAPIC Incident data template and work with NGIC Extract/Transform/Load (ETL) tools to facilitate import of JTAPIC accident and aviation data
- Run specialty queries for analysts/users
- Run queries and provide outputs in support of CIAD and JTAPIC monthly metric reporting requirements
- Implement CCB-approved changes for data values, migrating data from old values to new values
- Monitor implementation of ad hoc data fields within CIDB and nominate fields to the CCB for movement from ad hoc to permanent tables with each release
- Monitor deprecation of fields within CIDB and nominate columns for permanent removal in a release after waiting two releases after deprecation

The following deliverables are applicable to PWS Section 6.3:

- CIDB/JDB Data Administration guide
- JTAPIC Data Import Guide
- Updates to the CIDB and JDB Data Dictionaries, as required

6.4 Operations and Maintenance – Task 4

The Contractor shall ensure the CIDB and JDB are continually updated and maintained to remain viable for network operation and as customer business rules change. The Contractor shall ensure continued application compliance with changing guidance based on DoD Intelligence Community (IC) or Army mandates and directives. The Contractor shall provide maintenance to the CIDB and JDB IAW the NGIC SDLC policy and ISO/IEC 14764 guidance.

Due to the changing nature of mission requirements, the vendor should plan to implement the high level requirements listed in the following PWS subsections (or similar scoped requirements as prioritized by the CJDB CCB) during the course of the period of performance of the base year. The maintenance releases shall follow the procedures identified in PWS 6.1.8, Release Management.

6.4.1 Corrective Maintenance. The Contractor shall support corrective maintenance of the CIDB and JDB. Corrective maintenance refers to modifications necessitated by actual errors in the software products (i.e., defects/bugs). If the software product does not meet its requirements, corrective maintenance is performed. Corrective maintenance also includes implementation of Information

Assurance Vulnerability Alerts (IAVA) fixes. The maintenance releases shall follow the procedures identified in PWS 6.1.8, Release Management.

The Contractor shall provide Emergency releases to mitigate a critical information assurance vulnerability, and when standard application performance is impacted due to an unanticipated issue that stops mission productivity, with no readily identified and/or approved workaround. The emergency release should return the software application to its intended state. An emergency release occurs between version releases and contains no new functionality. For Emergency releases, a negotiation will occur between the Contractor and the Government regarding scope and schedule of the current releases in work in order to support the remedy of the degraded application. Emergency releases shall be documented and released using the NGIC SDLC Patch Release Process.

If a work around is available, the Contractor must gain approval from the functional representative and TTM to proceed without an Emergency release. If the workaround is approved, the Contractor should work each fix into the release cycle for the next scheduled production release. The emergency patch release process is only to be leveraged in a true emergency where no acceptable work around exists and the issue is causing unacceptable performance for the stakeholder.

6.4.2 Preventive Maintenance. The Contractor shall support preventive maintenance of the CIDB and JDB. Preventive Maintenance refers to the modifications necessitated by detecting potential errors in the software products, such as refactoring aspects of the application to ensure continued sustainability and scalability. The following is for estimating purposes only regarding the base period of performance tasks that are to be addressed through preventive maintenance activities:

- Affects both CIDB and JDB
    - Evolve the Mid-tier architecture to include connection pooling, STIG-compliant error handling mechanisms, server side data validation, and movement of application logic from the persistence layer (i.e., database) to the mid-tier
    - Separate the existing CIDB into three components (CIDB application, JDB Application, and Common Code Libraries) in order to create a more modular and scalable application architecture that facilitates independent release schedules for the CIDB and JDB.
- CIDB
    - Integrate with the NGIC Enterprise Content Management system to store media attachments for incident records. Migrate existing attachments from the current file folder construct to the content management system. Support an interface with incident triage or ETL tools so that associated file attachments are stored during initial incident record creation. Enable access to incident file attachments to remote users.
- JDB
    - Refactor the current execution of the Role Based Access Control (RBAC) feature from using logic in oracle (Virtual Private Databases) to utilize the NIST-compliant application logic in the mid-tier
    - Refactor the current audit feature so that data records are initially baselined and only changes to records are securely recorded. Audits should also capture user actions, user access to data and application administration actions. Overall the system audit footprint and resource cost should be lowered

6.4.3 Adaptive Maintenance. The Contractor shall support adaptive maintenance of the CIDB and JDB. Adaptive modifications are those modifications necessary to accommodate a changing environment. Adaptive modifications include modifications to implement new system interface requirements, new system requirements, or new hardware requirements. Adaptive maintenance also includes updating the

CIDB and JDB to maintain compliancy with the most current Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) for the technology leveraged by the CIDB and JDB. Adaptive maintenance also includes upgrades to the existing system architecture as the NGIC Standards and Architecture guidelines are modified (e.g., upgrading application server, operating system, and/or database software versions).

6.4.4 Perfective Maintenance. The Contractor shall support perfective maintenance of the CIDB and JDB. Perfective modifications improve the software product's performance or maintainability. A perfective modification might entail providing new functionality improvements for users. The following is for estimating purposes only in the base period of performance that are to be addressed through perfective maintenance activities:

- CIDB
  - Add Munition as a data object within the Incident record
  - Increase usability for concurrently adding (i.e., bulk add) and displaying multiple data objects
  - Update the CIDB Incident context interface to provide a graphical mean for analysts to create relationships between data objects
  - Implement dashboards so that users can create personal or team-based work queues to manage incident processing efforts
  - Update RBAC to implement a read-only CIDB role
- JDB
  - Implement dashboards within the JDB so that the user can visualize data coverage and/or data integration work queues within the JDB
  - Provide a Customer feedback mechanism within the JDB to capture a user's feedback while using the application
  - Support addition of JTAPIC Accident and Aviation data, leveraging an ETL capability such as Pentaho
- GRAIL
  - Update RBAC to implement an IED Analyst role
  - Support the ability to launch a search of NGIC's SPIRIT application using the DoD equipment code within CIDB
  - Add fields within the CIDB to capture the discovery of weapon caches
  - Support the ability to launch the CIDB flexible search from NGIC's SPIRIT application to find incidents based on the DoD equipment code

NOTE: The Contractor shall not load any unapproved software without the written permission of the COR & TTM listed in the PWS to the NGIC Environments.

The following deliverables are applicable to PWS Section 6.4 and all of it's subsections:

- Software with Source Code and Change Documentation
  - Emergency Patch Releases
- Validated software releases to NGIC Pre-Production/UAT Network(s)

6.5 Requirements Management – Task 5

6.5.1 Requirements Planning and Collection. The Contractor shall prepare and deliver a high-level Requirements Management plan. The plan shall outline the Contractor's specific approach and timeline used to collect and manage requirements.

The Contractor shall work with the COR & TTM, designated Subject Matter Experts (SME) and government designee support to collect system requirements for the CIDB and JDB. System requirements as defined in section 6.4 will be analyzed and approved for scheduled releases at Configuration Control Board (CCB) meetings, as part of the Weekly IPT. The Government shall have full access to the change tracking tool to review requirements at their discretion. The Contractor shall capture and track requirements in the change tracking tool (i.e. Jira) and shall contain the following fields for each requirement at a minimum:

- Title
- Requestor
- Requestor Organization
- Date Requested
- Description
- Mission Justification
- Technical Approach
- System Impact
- Associated Risks
- Recommended Priority
- Recommended Release
- Acceptance Criteria

Additional Artifacts to be attached to the each requirement:

- When the requirement introduces a change to an existing data flow within the system, provide an updated data flow diagram
- When the requirement is for a new feature, provide associated user story(ies) and/or wireframes
- When the requirement supports updated, modified, or previously undocumented business process(es), provide business process flow diagram(s)
- When the requirement introduces or changes existing system interfaces, provide updated DoD Architecture Framework (DoDAF) diagram(s) as required by the SDLC

The Contractor shall collect requirements per high level features identified by Government or designated representative as described in PWS section 6.4 and all associated PWS Subsection. The Contractor shall capture and manage all requirements in an automated requirements management tool. In addition to the user community, functional requirements may originate from Enterprise Service Center (ESC). On a monthly basis, the Contractor shall review all CIDB related ticket items and capture those items that introduce new system requirements.

During the CCB, the Contractor shall report on the new requirements using the change tracking tool at which point the Government will review and prioritize requirements for the next release. Additionally, the Contractor will provide the number of system requirements not yet analyzed, and number of requirements awaiting review.

The following deliverables are applicable to PWS Section 6.1 and all of it's subsections:

- Requirements Management Plan
- Requirements maintained in a change tracking tool

6.6 Information Assurance – Task 6

The Contractor shall support the NGIC Cyber Security Office or Government Designee on the following activities:

1) Provide input to the creation/update of the CoN package

2) Respond to NGIC Cyber concerning findings from the NGIC required scans
3) Ensure continued compliance with the DISA Application and Development STIG

6.7 Government Directed Surge (Optional – This Task Is A Labor Hour Contract Type):

It is anticipated that the Government may require the Contractor to surge resources to support requirements under PWS Section 6.0 (inclusive of all PWS subsections) of this Task Order. The contractor shall support these requirements, while continuing to provide the standard contracted FFP requirements. It should be noted that optional government directed surge may apply to any mandatory tasks under Section 6.0 of this TO.

For proposal and estimating purposes only, the Not-to-Exceed (NTE) value of this option is 10% of proposed labor for each period of performance.

Government directed surge should only be used when all other possibilities have been exhausted. Surge costs shall not be incurred unless authorized by the Contracting Officer (CO) and unless funding is available to cover incurred expenses.

At the time of exercising this optional support, at a minimum the Government shall

- Identify the event which is driving the surge requirement
- Identify the specific services where surge is authorized
- Utilize the labor rates for that specific year (e.g. base period or option period) and specific labor category
- Define level of effort expectations
- Identify duration or end date when surge is no longer required
- Provide an estimate on the number of surge hours required.

7. Acceptance Plan.

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the Quality Assurance Surveillance Plan (QASP)

7.1 Performance Standards. This section captures the outcomes that the NGIC seeks to achieve through this task. This section documents those performance measures and management processes that monitor and compare actual performance to planned results. Table 7-1 lists contractual performance standards. Acceptable Quality Level (AQL) Mission Success Ratings for all deliverables in Table 7-1 below are:

Exceptional: 95%-100%
Very Good: 85%-94%
Satisfactory: 75%-84%
Marginal: 70%-74%
Unsatisfactory: 69% and below

Table 7-1 Performance Requirement Summary (PRS)

The columns are defined as follows:

- PWS Section - Indicates the corresponding PWS section.
- Performance Standard - Provides a description and context for which the performance measure will be calculated.

- Method of Surveillance - Indicates the primary technique for monitoring and evaluating performance.
- Acceptable Quality Level (AQL) - The agreed upon performance level that is acceptable to the Government for a given performance measure.
- Incentive - Monthly payment shall be held until Acceptable Performance Level or mitigation plan is accepted by COR.

PWS Section inclusive of Subsections	Performance Standard	Method of surveillance	Acceptable quality level (AQL)	Incentive
6.1 Task 1 – Technical Management	a. **Technical** Deliverables must be 100% complete and on time. b. Any changes to initial plans and reports are: a. Communicated to the COR immediately b. Documented in original plan Documented in the MSR	100% Inspection of deliverables. Review of Daily, Weekly, Monthly, and Quarterly Reports, Emails, communication, customer complaints, inspections, and/or evaluations. Random inspection.	95% of deliverables are met on-time. 70% of deliverables are accepted on first submission without changes or clarifications by the COR or functional representative.	Monthly payment shall be held until Acceptable Performance Level or mitigation plan is accepted by the COR. 1% of current PoP value shall be subtracted from award for each Contractor calendar week Contractor is below Acceptable Performance Level or mitigation plan is not accepted by the COR.
6.2 Task 2 – Applications Administration	Contractor shall provide on-site support to the customer regarding CIDB and JDB activities such as role management, application configuration, Strike Point drawings, user manuals, and others as identified in the PWS.	Customer satisfaction as measured through limited validated customer complaints and feedback. Random Inspection of daily metrics reports. Implementation of changes to default report formats in Pentaho as requested/ approved by the government.	90% compliance with daily metrics report updates. 100% of changes to default custom reports implemented within 10 business days of request unless deviation is presented and approved by the COR and functional representative.	Monthly payment shall be held until Acceptable Performance Level or mitigation plan is accepted by the COR.
6.3 Task 3 – Data Administration	Contractor shall provide on-site support to the maintenance of data within CIDB and JDB including pick list values, supporting ad hoc query requests, successful data import from external data sources, and other items as described in PWS IAW Task 3	Customer satisfaction as measured through limited validated customer complaints and feedback. Pick list value changes implemented as reviewed and approved by the government at the CCB. Data import tasks completed in a reasonable timeframe after request with mapping to software releases for any database and UI changes required for import. Ad hoc queries returned to the government within 5 business days of request. Deviations can be approved at the government's discretion (e.g., government must respond to an RFI in 24 hours, therefore query results must be returned sooner).	100% of pick list value changes met during the year. 85% data import and migration tasks met for the year. 90% of queries returned at, or before, the specified deadline.	Monthly payment shall be held until Acceptable Performance Level or mitigation plan is accepted by the COR. TO

6.4 Task 4 – Applications Operations and Maintenance	a) Deliverables must be 100% complete and on time. b) Working software is the primary measure of progress. c) Priority is to fulfill customer business needs by: a. adaptive planning, b. technically sound architectures, requirements, and designs, c. frequently provide, working and valuable software, d. continuous and sustainable software improvement and development, e. rapid and flexible response to customer change of needs, f. continuously working with customer to define business needs, and g. accurately documenting current and future customer needs. d) Documentation, prioritization, and communication of correction maintenance required to the COR and functional representative(s) at CCB. e) All modifications and updates to the software product are in compliance with cybersecurity vulnerabilities/guidelines. f) Current application functionality must be 100% maintained. g) All issues within a release are 95% identified prior to 1st sprint of that release. h) Maintain and sustain SPIRIT software applications in accordance with NGIC SDLC policy, NGIC IT standards, and DOD best practices. i) Software deliverables must be uploaded to appropriate networks for deployment. j) Deliver software releases in accordance with IMS quarterly.	Prior to delivery of software releases to NGIC Production networks, the Contractor shall be required to demonstrate the operational capability of the system software in NGIC Test and PreProduction Networks. This capability is further validated by running security scans of the server containing the application and will be reviewed by the government for compliance. Customer satisfaction as measured through limited validated customer complaints and feedback.	All requirements mandated by law or regulation must be 100% compliant. Any deviation must be identified with approved mitigation and plan of action and milestones (POA&M). 95% On-time delivery of three (3) software releases. 95% of final software releases require 2 or less minor patches. 90% Of items listed in the release planning are included in the actual release. Software releases containing defects (e.g., security or functionality) identified through testing will be reviewed by the government to determine if they are acceptable in Production, or if they must be resolved before a Production deployment. Any defects deemed unacceptable must be resolved in 10 business days and resubmitted for verification of resolution prior to deployment to production.	100% payment for meeting all mandated requirements. Nonconformance with minimum specified requirements is unacceptable. Payment is withheld until the software is validated and approved by the customer to move to Production. Validation occurs in the PreProduction environment. Payment will be reduced for any software release that does not meet the government confirmed deployment schedule: 1% of the current PoP value per week schedule slip.
6.1 & **6.5 Task 5 – Requirements Management**	Contractor's management of CIDB and JDB requirements conforms to PWS stipulations and requirements tracking tool/reports are accessible to the government COR.	Validated requirements updated/estimated/prioritized in requirements tracking tool as evidenced by weekly CCB and per government's request to review CIDB and JDB requirements.	90% of all CIDB and JDB requirements for implementation in each software release shall be estimated for level of effort and planned technical design/ implementation prior to beginning a development cycle.	100% payment for meeting all mandated requirements. Development on any requirement will not be authorized until the AQL is met, potentially affecting successful ability to meet requirements IAW Task 4.

			50% of all CIDB and JDB backlog items shall be estimated for level of effort and high level technical implementation prior to the end of the current year period of performance.	
6.6 Task 6 – Information Assurance	Contractor shall ensure CIDB and JDB are developed to meet cyber security requirements and support input to creation or update of the Certificate of Networthiness (CoN) requests.	Evidenced by software release implementation through passage of security scans and quick response to requests for assistance completing accreditation documentation.	100% compliance with regulatory and cyber security guidance.	100% payment for meeting all mandated requirements.

8. **Incentives**. See Table 7-1

9. **Place of Performance**.
The primary place of performance shall be at the NGIC facilities.

a. NGIC facilities - Charlottesville, VA
b. Contractor Facilities – TBD

10. **Period of Performance (PoP)**. The PoP for this task order is for a one-year base period from time of award and three consecutive one-year option periods.

11. **Delivery Schedule**. The Contractor shall provide all documentation deliverables in softcopy by email to the COR and TTM before 1545 ET on the due date. The Government will review the deliverables within ten (10) business days unless otherwise specified in the Performance Standards Summary, table 7-1. If comments need to be incorporated, the Contractor has 5 business days to incorporate and resubmit for approval.

Standard Distribution: NGIC Local Technical Task Monitor, NGIC Functional Representative

11.1 **Deliverables Schedule**

PWS Task#	Deliverable Title	Format	Number	Calendar Dates after TO start
1	Task Order Management Plan (TOMP)	Contractor determined format IAW PWS	Standard Distribution	Initial - 30, Updates as necessary with MSR
1	Integrated Master Schedule (IMS)	Contractor determined format IAW PWS	Standard Distribution	Initial - 30, Updated by the 10th workday of each month
1	Monthly Status Report (MSR)	Contractor determined format IAW PWS	Complete Copy to COR & TTM; Transmittal Letter (TL) only to KO	Monthly, NLT 10th Workday
1	Weekly Integrated Project Team Meeting	CCB presentation – Contractor determined format IAW PWS; supports Functional Representative's creation of meeting agenda	Standard Distribution	Weekly; Agenda NLT 2 workdays prior; Notes NLT 2 workdays after
1	In-Process-Review Briefing	Contractor determined format IAW PWS	Complete Copy to COR & TTM; Transmittal Letter (TL) only to KO	Quarterly, with draft IPR slides delivered 5 business days prior to scheduled date; final materials delivered ~~5~~ 1 business day~~workdays~~ prior to scheduled date. Agenda NLT ~~7 workdays~~5 business

				days prior; Notes NLT 5 workdays after
1	Risk Mitigation Plan (RMP)	Contractor determined format IAW PWS	Standard Distribution	Initial - 30, Updates as necessary with MSR
1	Quality Management Plan (QMP)	Contractor determined format IAW PWS	Standard Distribution	Initial - 30, Updates as necessary with MSR
1	Metrics Report	Contractor determined format IAW PWS	Standard Distribution	Initial – 30, Updates with software release
1	Software Configuration Management Plan (SCMP)	Contractor determined format IAW PWS	Standard Distribution	Initial - 30, Updates as necessary with MSR
1	Release Package	Contractor determined format IAW PWS	Standard Distribution	Every software release; once prior to starting work on release and any updates necessary to achieve signature, and once post successful UAT for signature
1	Application User Manual/Guide	Contractor determined format IAW PWS and specific to each application (i.e., CIDB User Manual and a JDB User Manual)	Standard Distribution	Every software release as application functionality is updated
1	Software Release Documentation from SDLC Volume as determined by scope of release	IAW NGIC SDLC Templates	Standard Distribution	NLT 3 business days before scheduled maintenance window
1	Documented Coding Standards and Development Processes	Contractor determined format IAW PWS	TTM	Initial – 60, Updates as necessary
2	CIDB/JDB Account SOP	Contractor determined format IAW PWS	Standard Distribution	Initial – 60, Updates as necessary
2	Configuration guide	IAW NGIC SDLC Templates	Standard Distribution	Updates as necessary – required for CoN submission
2	Run Book	IAW NGIC SDLC Templates	Standard Distribution	Updates as necessary and with each software release
2	System Administration Guide	IAW NGIC SDLC Templates	Standard Distribution	Updates as necessary
2	Daily Application Metrics	Contractor determined format IAW PWS	TTM	Consolidation of metrics delivered twice monthly via email
3	CIDB/JDB Data Administration Guides	Contractor determined format IAW PWS	Standard Distribution	Initial – 60, Updates as necessary
3	JTAPIC Data Import Guide	Contractor determined format IAW PWS	Standard Distribution	Initial – 60, Updates as necessary
3	Updates to JDB Data Dictionaries	Maintain Existing Data Dictionary Format	Standard Distribution	As necessary
4	Emergency Patch Release Software with Change Documentation	Contractor determined format IAW NGIC Change Management Process	Standard Distribution	NLT the day of Patch release deployment
4	Emergency Patch Release Documentation	IAW NGIC SDLC Volume 5	Standard Distribution	NLT 7 calendar days after the day of Emergency Patch release deployment
4	Software with Change Documentation	Contractor determined format IAW NGIC Change Management Process	Standard Distribution	NLT 2 business days before scheduled installation into expected environment (Test, Pre-Production)
4	Validated software releases to NGIC Pre-Production/UAT Network(s)	Contractor shall deliver the specified number of releases per application as stipulated in the PWS.	Standard Distribution	Per Release Package and NLT 3 business days before scheduled maintenance window
5	Requirements Management Plan	Contractor determined format IAW PWS	Standard Distribution	Initial - 30, Updates as requested by Government TTM

5	Requirements managed in a change tracking tool	Contractor determined format IAW PWS	TTM and Functional Representative	Always up-to-date and available for review

11.2 Payment Schedule

Deliverable	**Percent of Price Contractor is authorized to bill for**
Monthly MSR	6% per MSR
Software release and SDLC package	9% of total
Software release and SDLC package	9% of total
Software release and SDLC package	10% of total

12. **Security**. DD Forms 254: Overarching security requirements and Contractor access to classified information shall be as specified in the basic DD Form 254. All Contractors whose place of performance (see Section 9 above) require TOP SECRET, SCI with additional compartments at time of award in order to have unescorted access to the NGIC. All Contractor staff working on this effort shall have a DOD Secret clearance prior to charging to this effort.

12.1 Personnel Security Clearances. IAW the DD254, all Contractor employees working on-site at NGIC/Rivanna Station shall possess a minimum of a Top Secret/SCI clearance.

12.2 Reports of Adverse Information. The Contractor shall report to the NGIC Security Manager all adverse information on Contractor personnel, such as security violations, arrests, bankruptcy, and denial, suspension, or revocation of security clearances. The NGIC Security Manager, based upon the adverse information, may recommend that the NGIC Commander deny an employee access into NGIC restricted areas. The Government reserves the right to direct any Contractor employee to be removed for performance, directly or indirectly, whenever there is probable cause to believe, that such action is warranted in the interest of national security. This action shall be made whether or not the cause is deemed of sufficient severity to warrant action to terminate the Contractor.

12.3 Security Badges. Security badges will only be issued to Contractor personnel IAW NGIC policy. NGIC's Security personnel will approve and issue security badges to Contractor personnel upon written request from the CJDB COR and after the investigation or security clearance has been verified by CSE. Contractor personnel shall wear the security badge at all times when in the restricted areas of NGIC/Rivanna Station.

12.4 Automated Information Systems (AIS) Access. Contractor personnel requiring access to NGIC AIS shall meet the personnel security standards IAW paragraph 2-16, Army Regulation (AR) 380-19. The required investigations must be favorably completed prior to employees being permitted access to NGIC AIS. The Contractor shall ensure that all NGIC AIS used by Contractor personnel are protected and accredited IAW applicable directives. NGIC will provide AIS security support to Contractor personnel using NGIC computers.

12.5 CAC/Internet Access: Contractor employees assigned to this task order are required to obtain a Common Access Card (CAC) in order to retrieve Government provided internet/intranet information.

12.6 Installation Access. Most of these functions are performed in the restricted area of NGIC/Rivanna Station. All vehicles and personnel are subject to search and seizure of contraband and/or unauthorized Government property IAW AR 190-13. All Contractor personnel will comply with NGIC/Rivanna

Station requirements for movement within the Installation: entry, exit, and internal control of personnel, material, and vehicles at NGIC/Rivanna Station. The CJDB COR will approve and arrange via written request for the NGIC Security Office to issue a NGIC Security Access Badge to enable Contractor personnel, whose regular duty station is at NGIC, to gain access to NGIC. Contractor personnel shall display this badge to on-duty security personnel at the entrance gates to gain access to NGIC/Rivanna Station.

12.7 Foreign Nationals/Immigrant Aliens. Foreign nationals/immigrant aliens cannot be granted unescorted access to the work-site, and shall not be scheduled to perform work under this TO. However, when foreign nationals/immigrant aliens are visiting NGIC, the Contractor shall comply with NGIC Policies and AR 380-10.

12.8 Safeguarding Government Information and Property**.** The Contractor shall be responsible for safeguarding all Government information and property provided for Contractor use. The Contractor shall safeguard information and material designated as classified, unclassified sensitive, For Official Use Only (FOUO), Operations Security (OPSEC) sensitive, and Privacy Act Information IAW applicable directives. NGIC will provide copies of appropriate directives and security classification guides as required. Security violations will be dealt with IAW with paragraph 2-16, AR 380-19.

12.9 Loss or possible Compromise of Classified Information. The Contractor shall immediately report the loss or possible compromise of classified information or material to the NGIC Security Manager or his designee, IAW NGIC policies. This report shall also be sent to the CJDB COR and TTM.

12.10 Key Control. The Contractor shall have access twenty-four (24) hours a day, seven (7) days a week to all Government-furnished facilities IAW AR 190-51 and NGIC Policies. The Contractor shall ensure that metal and electronic keys received from the Government are accountable, controlled, and safeguarded IAW the two regulations just cited.

12.11 Lock Combinations – The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Contractor’s Quality Control Plan (QCP).

12.12 Security Training. The Contractor shall develop and implement a security education program to insure Contractor personnel understand and are familiar with security requirements. The Contractor shall conduct security indoctrination for all new employees within thirty (30) days after their arrival, and refresher sessions annually thereafter. This training will include general security education, OPSEC awareness, Information Systems Security, Force Protection, and training on Subversion and Espionage Directed Against the Army (SAEDA)/Threat Awareness Reporting Program (TARP).

12.13 Operations Security (OPSEC).

12.13.1 Operations Security (OPSEC): AR 530-1, 19 April 2007, Training Programs. The Contractor shall provide OPSEC training to all employees regarding the safeguarding of sensitive information prior to employees being allowed access to such information. Chapter 4 of AR 530-1, Training, requires that newly arrived personnel receive an OPSEC orientation briefing within the first 30 days of arrival at the organization. The AR further requires that all personnel receive an annual OPSEC briefing. Contractor personnel may utilize the OPSEC briefings presented by the INSCOM OPSEC Program Manager/Coordinator. The Contractor will submit certificates of completion or sign in rosters all initial and annual OPSEC training to the COR.   The above requirements will flow down to all Subcontractors working on or providing support to the TO.

12.13.2 The Contractor shall not release sensitive information to the general public without prior written approval from the Contracting Officer. All Contractor requests to release sensitive information shall be in writing and clearly explain the necessity for release of the information and consequences if approval is not granted.

12.13.3 All material produced by the Contractor which will be released to the general public will be subject to OPSEC and Security reviews from INSCOM OPSEC Officer, Security Officer and INSCOM Public Affairs Office prior to release.

12.13.4 The Contractor shall destroy all sensitive program material at the completion of the TO so as to ensure the information cannot be accessed or utilized for any purpose. The Contractor will also notify the Contracting Officer in writing of its destruction. These same requirements will flow down to all Subcontractors working on or provided any sensitive information related to the TO.

12.13.5 Per AR 530-1, Operations Security, new Contractor employees must complete Level I OPSEC training within 30 calendar days of their reporting for duty. All Contractor employees must complete annual OPSEC awareness training.

12.14 Departing Employees. The Contractor shall ensure all Contractor employees return security identification badges and picture identification cards (e.g., Common Access Cards) to the Government at the completion of their employment.

12.15 Additional Security Requirements: This effort requires access to classified Government information at U.S. Government facilities only. Physical, personnel, information and operational security measures are part of the security specifications for this order as outlined in the DD Form 254 IAW DIAM 50-5 and all other Government security regulations, manuals and directives. Additional requirements are contained in the DD Form 254.

13. **Government Furnished Property (GFP).**

Government Furnished Property (GFP) includes Government Furnished Information (GFI), Government Furnished Equipment (GFE) and Government Furnished Material (GFM). All existing and relevant GFI, which includes documents and procedures regarding the performance of this TO, will be provided by the Government within 30days after TO award.

Government Furnished Equipment (GFE) includes Property, Plant and Equipment (PP&E) (equipment, machine tools, test equipment, etc), Special Test Equipment (STE), and Special Tooling (ST). GFE to be provided to the contractor shall consist of office space, office equipment, computers, phones, office supplies, and LAN/Internet access for those tasks performed on site. Note: Cell phones (and conference lines others than those provided) are not authorized or allowable as an ODC under this TO.

All GFP distribution, location, and inventory shall be tracked by the contractor. The contractor shall make this tracking information available to the government as needed. Unless otherwise specified, all GFP will be returned at the completion of the TO. Note: if contractor requires additional GFP other than what is listed, the contractor shall submit a request to the COR within 30 days after TO award.

14. **<u>Other Pertinent Information or Special Considerations</u>**.

14.1 <u>Identification of Possible Follow-on Work</u>. The options are exercised at the discretion of the Government and are also contingent upon funding.

14.2 <u>Incorporate the appropriate DOD-mandated architecture programs, standards and guidelines</u>. The following references are required: DoDAF, Joint Technical Architecture – Army (JTA-A), Director of Central Intelligence Directives (DCID) 6/3 Common Criteria, Intelligence Community Directive (ICD) 503, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02B, Executive Order 12333, the Intelligence Oversight provisions of AR 381-10, U.S. Army Intelligence Activities, Joint Requirements Oversight Council (JROC), Joint Capabilities Integration and Development System (JCIDS), Army Requirements Oversight Council (AROC), Defense Intelligence Integrators Guide (DIIG) version 1.2, date 2/15/2007 and NGIC Regulation 5-3. The Information Technology Process at NGIC: the NGIC SDLC, NGIC Change Management Process.

14.3 <u>Identification of Non-Disclosure Requirements</u>. Contractors shall execute non-disclosure agreements when they work with sensitive and/or proprietary information. This task will involve sensitive planning for subsequent systems acquisition and enhancements. Therefore, non-disclosure agreements will be required at the time of award.

14.4 <u>Identification of Possible Significant Growth</u>. The level of effort for the various tasks outlined in the PWS may be expanded by number of labor hours and/or labor categories as required in the performance of the PWS.

14.5 <u>DoD Directive (DoDD) 8570.01-M Compliance</u>. The Contractor must maintain personnel at DoDD 8570.01-M compliance per functional role. All Contractors whose functional role is specified as IAT I, II, III or IAM I, II, III, must meet training requirements established in DoDD 8570.01-M at time of award. Certification requirements are identified in the following:
http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf and
http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html#baseline-cert.

14.6 <u>Transition</u>. The Contractor shall support a thirty (30) day transition-in period from date of task order award. The contractor shall support a transition-out period consisting of 45 days prior to contract end date to allow for orderly contract transition. The transition-in and transition-out periods are inclusive of existing periods of performance.

Throughout the transition-in/transition-out periods, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission. The contractor must plan for the transfer of work control, delineating the method for processing and assigning tasks during the transition-in/transition-out periods.

14.6.1 Transition-In Plan. The Transition-In Plan shall contain, at a minimum:

- Transition-in activities,
- Risks Management,
- Schedules and Milestones for transition-in activities,
- Staffing plan, to include on boarding process
- Ability to attract, recruit, and retain qualified personnel and its ability to quickly and effectively respond to contingency requirements
- Ability to obtain and process security clearance,

- Security Clearance
- Approach to achieving 100% of the Firm Fixed Price manning requirements by the conclusion of the transition period.

Immediately after award of the task order, the winning contractor shall initiate contact with the government and jointly review a draft transition-in plan. The Contractor shall support an initial meeting between the Government's Contract Administrator and Contract Managers to maximize the effectiveness of the transition process no later than seven (7) working days of the task order award. This meeting shall address the Contractors transition-in requirements and responsibilities concerning the Transition-In Plan. The contractor shall then revise the transition plan, if necessary, and submit the final plan within ten (10) working days of task order award. Subsequent meetings shall be held as determined by the Contracting Officer, but not less than weekly thereafter.

The contractor's final approved plan shall provide for the full transition within thirty (30) days of task order award. All changes to the schedule must be communicated to the COR. During the transition-in period, personnel may be permitted to observe operation of the contractor and Government pertaining to this contract, subject to approval by the Government COR.

14.6.2 Transition-Out Plan. The Contractor shall develop a transition-out plan to affect a smooth and orderly transfer of contract responsibility to a successor. The plan shall fully describe the outgoing Contractor's approach to the following issues, at a minimum, IAW DI-MGMT-80004A, subtitled, "Transition-Out Plan."

Inventories and turn-over of government property; removal of Contractor property; reconciliation of all property accounts; turn-in of excess property; data and information transfer (inclusive of current documentation and historical records); clean-up of Contractor work areas; security debriefings IAW AR 380-5 for incumbent personnel holding security clearances; work-in-progress; and any other actions required to ensure continuity of operations.

The Contractor shall provide a draft of the plan to the COR sixty (60) working days before the phase-out period commences. The Contractor shall support a meeting between the Government's Contract Administrator and Contract Managers to maximize the effectiveness of the transition process no later than forty-five (45) days before the phase-out period commences. This meeting shall address the Contractors transition-out requirements and responsibilities concerning the Transition-Out Plan. The contractor shall then revise the transition-out plan, if necessary, and submit the final plan within thirty (30) working days before the phase-out period commences. Subsequent meetings shall be held as determined by the Contracting Officer, but not less than weekly thereafter.

Prior to the completion of this contract, an observation period shall occur, at which time team management personnel of the incoming Contractor may observe operations. This will allow for orderly turnover of facilities, equipment, and records and will help to ensure continuity of services. The outgoing Contractor is ultimately responsible for performing full services IAW the contract, during the transition-out period, and shall not defer any requirements for the purpose of avoiding responsibility or of transferring, such responsibility to the succeeding Contractor. The outgoing Contractor shall fully cooperate with the succeeding Contractor and the Government, so as not to interfere with their work or duties.

To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the outgoing Contractor shall have all personnel on board during the phase-out period. The outgoing Contractor shall be prepared to transition the workload to the newly selected Contractor during the forty-five (45) day transition-out period, which will occur at the end of the period of performance of the contractual effort

14.6.3 The Facility Security Officer (FSO) must provide to HQ INSCOM/Major Subordinate Command (MSC) COR, the following information on all Contractor Manpower Equivalents (CMEs) performing HQ INSCOM/MSC missions and are direct labor, for input into the INSCOM In/Out Processing Portal.

In Processing	Out Processing
Contractor Name	Contractor Name
Contractor Email	Contractor Email
Contractor SSN (Full)	Contractor Phone Number
Contracting Company	Contractor SSN (Last 4 Only)
FSO Email	INSCOM Organization
Hours at HQ INSCOM/MSC	Contract Number
Percentage on Contract	Contracting Company
Contract Number	FSO Email
PoP End Date	Departure Date
Paragraph	Separation Type (drop-down)
Line Number	Transfer Type (drop-down)
UIC	COR (populated automatically)
Arrival Date	
HQ INSCOM/MSC Organization	
COR (populated automatically)	
IT POC (selected from HQ INSCOM/MSC population)	

14.6.4 All CMEs directly allocated to a HQ INSCOM/MSC TO will be In/Out processed through the HQ INSCOM/MSC In/Out Processing Portal by the respective COR, with the assistance of information provided by FSO.

14.6.5 All CMEs directly allocated to a HQ INSCOM/MSC TO must be Read-On/Read-Off by a Security Specialist at an HQ INSCOM/MSC facility.

14.6.6 CMEs will **NOT** be Read-On/Read-Off and facility access will **NOT** be granted if the required information has not been entered into the HQ INSCOM/MSC In/Out Processing Portal prior to arrival and prior to departure. In the instance of Out Processing, this may affect CPARS reporting on your organization.

14.6.7 CMEs will complete Information Assurance (IA) Training (required for Government systems access), and obtain a completion Certificate prior to Entry On Duty (EOD). The completion Certificate will be sent to the responsible COR to confirm compliance prior to EOD. Initially, non-CAC access to Army Knowledge Online (AKO) is required to complete IA training. However, CMEs must obtain a CAC prior to EOD.

14.7 Government Surveillance and Monitoring: The Contractor, not the Government, is responsible for the management and quality control actions to meet the terms and conditions of the TO. The role of the Government in quality assurance surveillance is to assess Contractor performance and to evaluate whether performance standards are achieved. It is the Contractor's primary responsibility to ensure all TO requirements meet required quality levels. The Government will ensure this responsibility has been met before payment is made to the Contractor.

14.7.1 Quality Assurance Surveillance Plan: A Quality Assurance Surveillance Plan (QASP) has been developed by the Government to provide a systematic surveillance method for the service rendered and which describes the methodology by which the Contractor's performance will be monitored. The QASP is a “living document” and the Government may review and revise it on a regular basis. The Government will coordinate changes with the Contractor. Updates shall ensure that the QASP remains a valid, useful, and enforceable document. Copies of the original QASP and revisions shall be provided to the Contractor and Government officials implementing surveillance activities upon TO award. Contractor performance will be evaluated utilizing the Contractor Performance Assessment Reporting System (CPARS).

14.7.2 Quality Control Plan: The QCP shall recognize the responsibility of the Contractor to carry out its quality control obligations and shall contain measurable inspection and acceptance criteria corresponding to the performance requirements of the PWS. The QCP shall focus on the level of performance required by the statement of work, rather than the methodology used by the Contractor to achieve that level of performance. The QCP shall specify all work requiring surveillance. The QCP shall specify the method of surveillance. The Government reserves the right to witness any and/or all surveillance at Contractor and/or government facilities, as may be necessary to determine that services conform to TO requirements.

14.8 Travel / Temporary Duty (TDY). No travel is required on this TO.

14.9 Staffing. The Contractor shall provide resumes, for Government review of qualifications and proposed levels of performance, of key personnel assigned to the task order. All personnel assigned must meet the qualifications of the TO Labor Category criteria they were hired for and billed against. Key personnel have been identified as the Project Manager, Software Engineering Lead, and Lead Database Specialist.

15. **Other Pertinent Information or Special Considerations**

15.1 Non-Personal Services. The Government shall neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual Contractor employees. It shall be the responsibility of the Contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the Contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the Contracting Officer (KO) immediately.

15.2 Business Relations. The Contractor shall successfully integrate and coordinate all activity needed to execute the requirement. The Contractor shall manage the timeliness, completeness, and quality of problem identification. The Contractor shall provide corrective action plans, proposal submittals, timely identification of issues, and effective management of Subcontractors. The Contractor shall seek to ensure customer satisfaction and professional and ethical behavior of all Contractor personnel.

15.3 Task Order Administration and Management. The following subsections specify requirements for TO, management, and personnel administration.

15.3.1 Task Order Management. The Contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement. The Contractor must maintain continuity between the support operations at 2055 Boulders Rd, Charlottesville, VA 22911 and the Contractor's corporate offices.

15.3.2 Task Order Administration. The Contractor shall establish processes and assign appropriate resources to effectively administer the requirement. The Contractor shall respond to Government requests for contractual actions in a timely fashion. The Contractor shall have a single point of contact between the Government and Contractor personnel assigned to support contracts or task orders. The Contractor shall assign work effort and maintaining proper and accurate time keeping records of personnel assigned to work on the requirement.

15.3.3 Personnel Administration. The Contractor shall provide for employees during designated Government non-work days or other periods where Government offices are closed due to weather or security conditions. The Contractor shall maintain the currency of their employees by providing initial and refresher training to meet the PWS requirements. The Contractor shall make necessary travel arrangements for employees. The Contractor shall provide necessary infrastructure to support TO tasks. The Contractor shall provide administrative support to employees in a timely fashion (time keeping, leave processing, pay, emergency needs).

15.3.3.1 Government Shutdown Requirements for Essential Contractor Personnel—24/7 Contract Coverage

a. Government Closure. In the event that the US Government Office of Personnel Management (OPM) officially announces closure of the federal Government, and federal employees (other than emergency essential personnel) are not required to report to work, the Contractor shall follow this guidance:

(1) Personnel who, in accordance with the terms of the contract, perform their contractual duties on a Government installation or in a Government facility, but have not been designated emergency essential personnel or are not fulfilling 24/7 requirements shall not report for duty under this contract and the contractor shall not invoice for those hours.

(2) Personnel who have been designated in writing by the Contracting Officer's Representative or verbally notified by the Contracting Officer (written confirmation will be provided within 2 business days) as emergency essential shall report to work.

(3) Personnel fulfilling 24/7 contract requirements (if any) who are not emergency essential but who are already at work may remain at work if approved by the Contracting Officer's Representative.

b. Installation Closure. The installation commander may, at his discretion, close the post, installation or facility even if the Government is otherwise open. In this case, (i.e., if the Government is open but the post, installation, or facility is closed), contractor personnel will not be able to report regardless of status. The Contractor shall not invoice for these hours. Unless a cognizant Government authority directs personnel to leave the installation, contractor personnel on site at the time of the closure may stay to complete their shifts at the discretion of the contractor manager taking into account safety and other issues. Contractors may bill for hours worked.

c. Announcements. The Contractor is responsible for monitoring announcements and informing employees of federal Government or installation closures.

d. Alternate Duty Sites. In the case of either Government closure or installation closure, the Contractor personnel whose place of duty is the installation or facility are not authorized to perform at an alternate duty site unless the Contracting Officer approves the type of work and the alternate location in writing in advance.

15.3.4 Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the contracting activity or TO administration office IAW Federal Acquisition Regulation (FAR) Subpart 42.5. The contracting officer (KO), COR, and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the KO will apprise the Contractor of how the Government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government.

15.3.5 Contracting Officer Representative (COR) and Technical Task Monitor (TTM): The COR monitors all technical aspects of the TO and assists in TO administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the TO; perform inspections necessary in connection with TO performance; maintain written and oral communications with the Contractor concerning technical aspects of the TO; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor the Contractor's performance and notifies both the KO and Contractor of any deficiencies; coordinate availability of Government-furnished property (GFP), and provide site entry of contractor personnel. A letter of designation is issued to the COR, a copy of which is sent to the contractor. It states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order. The Government may assign TTMs to assist the COR in monitoring the TO and reviewing deliverables. The TTM will also be the point of contact for Contractor inquiries and provide guidance, assistance and act as the liaison between the Contractor and the COR as necessary. The Government will assign TTMs for functional areas. The TTM will report to the COR and the COR will report to KO.

15.4 Subcontract Management. The Contractor shall be responsible for any subcontract management necessary to integrate work performed on this requirement and shall be responsible and accountable for subcontractor performance on this requirement. The prime Contractor will manage work distribution to ensure there are no Organizational Conflict of Interest (OCI) considerations. Contractors may add subcontractors to their team after notification to the KO or COR.

15.5 Contractor Personnel, Disciplines, and Specialties. The Contractor shall accomplish the assigned work by employing and utilizing qualified personnel with appropriate combinations of education, training, and experience. The Contractor shall match personnel skills to the work or task with a minimum of under/over employment of resources. The Contractor shall provide the necessary resources and infrastructure to manage, perform, and administer the TO.

15.6 Other Direct Costs (ODC): No contractor ODCs are required.

15.7 Training. The Contractor is required to ensure that all employees comply with the Mandatory Intelligence Training requirements for Contractor personnel IAWIAW AR 381-10. The Contractor must provide documentation to the COR that training has occurred for each employee. The training is mandatory for all personnel in the Intelligence environment.

15.7.1 Online Training. Mandatory online training includes 1) Anti-Terrorism Force Protection, 2) Combating Trafficking in Person, 3) Information Assurance, 4) Intelligence Oversight and 5) Annual Security Refresher Training. Additional training may be mandated by the Government.

15.7.2 Classroom Training. Mandatory classroom training includes 1) Classification Marking, 2) Operation Security (OPSEC) Initial Training, 3) OPSEC Annual Training and 4) The Threat Awareness and Reporting Program (TARP). Additional training may be mandated by the Government.

15.8 Antiterrorism Requirements.

15.8.1 Antiterrorism Considerations: IAW DFARS, 27 January 2011, 207.105(b) (20) (D), and DOD Instruction 2000.16, DoD Antiterrorism Standards, the Contractor is hereby advised that it shall comply with the policies and procedures of the U.S. Antiterrorism Officer (ATO) at each installation where work is being performed. DoD Instruction 2000.16 is available at the Washington Headquarters Services website at http://www.dtic.mil/whs/directives/. Information with regard to the INSCOM procedures and policies will be provided at a later date. A modification to the TO will be the instrument of notification for this action. The Contractor may submit a request for an equitable adjustment for any directly incurred costs for compliance with these policies and procedures, following the modification incorporating the policy and procedures guidance. Equitable adjustment requests shall be in compliance with clauses.

15.8.2 Antiterrorism and Force Protection (AT/FP): AR 350-1, 4 August 2011, Army Training and Leadership Development, Section II, G-7, Antiterrorism and Force Protection. Specific Army standards for AT/FP training are listed in chapter 5, AR 525-13, 11 September 2008. Individual AT/FP training is mandatory for all soldiers, Department of the Army civilians, and DOD contractors and is strongly recommended for family members prior to travelling outside the 50 United States and its territories and possessions for any reason, including mobilization, temporary duty, permanent change of station, and leave. There is also an AT/FP training requirement for personnel stationed outside the United States. Individual AT/FP training is valid for one (1) year and must be documented.

15.8.3 AT Level I Training: All contractor employees, to include subcontractor employees, requiring access to Army installations, facilities and controlled access areas shall complete AT Level 1 awareness training within 30 calendar days after TO start date or effective date of incorporation of this requirement into the TO, whichever is applicable. The Contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee to the COR/ACOR or to the contracting officer, if a COR/ACOR is not assigned, within 15 calendar days after completion of training by all employees and subcontractor personnel. AT Level 1 awareness training is available at the following website: https://atlevel1.dtic.mil/at.

15.8.4 AT Awareness Training for Contractor Personnel Traveling Overseas: This requires US based contractor employees and associated subcontractor employees to make available and to receive government provided area of responsibility (AOR) specific AT awareness training IAW by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.

15.8.5 Access and General Protection/Security Policy and Procedures: Contractor and all associated subcontractors employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements IAW DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this TO, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

15.8.6 iWATCH Training: The Contractor and all associated subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity Authorization to Operate (ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR/ACOR. This training shall be completed within 30 calendar days of TO award and within 30 calendar days of new employee's commencing performance. iWATCH training results shall be reported to the COR/ACOR not later than 45 calendar days after TO award.

15.8.7 Contractor Employees Who Require Access to Government Information Systems. All contractor employees with access to a Government information system must be registered in the Army Training Certification Tracking System (ATCTS) at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the Information System and then annually thereafter.

15.8.8 For information assurance (IA)/information technology (IT) certification. Per DoD 8570.01-M , DFARS 252.239.7001 and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon TO award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon TO award.

15.8.9 For Contracts that Require OPSEC Training. Per AR 530-1, Operations Security, new contractor employees must complete Level I OPSEC training within 30 calendar days of their reporting for duty. All contractor employees must complete annual OPSEC awareness training.

15.8.10 For Information Assurance (IA)/Information Technology (IT) Training. All contractor employees and associated subcontractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M, and AR 25-2 within six months of employment.

15.8.11 For Contracts That Require Handling or Access to Classified Information. The Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires Contractors to comply with the Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); and any revisions to DOD 5220.22-M, notice of which has been furnished to the Contractor.

15.9 Organization Conflict of Interest.

Performance under this task order may require the contractor to access data and information proprietary to a Government agency, another Government contractor or of such nature that its dissemination or use other than as specified in the work statement would be adverse to the interests of the Government or others. Neither the contractor, nor contractor personnel, shall divulge nor release data or information developed or obtained under performance of this work statement, except to authorized Government personnel or upon written approval of the contracting officer. The contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as specified in this work statement or any information at all regarding this agency.

Disclosure of Information regarding operations and services of the activity to persons not entitled to receive it and failure to safeguard any classified information that may come to the contractor (or any persons under the contractor's control) in connection with work under this work statement, may subject the contractor, contractor's agent, or employees to criminal liability under Title 18, sections 793 and 798 of the United States Code. Neither the contractor nor the contractor's employees shall disclose or cause to be disseminated, any information concerning the operations of the activity, which could result in, or increase the likelihood of, the possibility of a breach of the activity's security or interrupt the continuity of its operations.

The contractor shall direct to the contracting officer all inquiries, comments, or complaints arising from matters observed, experienced, or learned as a result of, or in connection with the performance of this task order, the resolution of which may require the dissemination of official information.

15.10 Contractor Manpower Reporting (CMR): The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where the Contractor shall report ALL contractor manpower (including subcontractor manpower) required for performance of this TO. The Contractor shall completely fill in all the information in the format using the following web address https://contractormanpower.army.pentagon.mil . The required information includes: (1) Contracting Office, Contracting Officer (KO), Contracting Officer's Technical Representative (COTR) or also known as the Contracting Officer's Representative (COR); (2) Contract number, including task and delivery order number; (3) Beginning and ending dates covered by reporting period; (4) Contractor's name, address, phone number, e-mail address, identity of Contractor employee entering data; (5) Estimated direct labor hours (including subcontractors); (6) Estimated direct labor dollars paid this reporting period (including subcontractors); (7) Total payments (including subcontractors); (8) Predominant Federal Service Code (FSC) reflecting services provided by contractor (and separate predominant FSC for each subcontractor if different); (9) Estimated data collection cost; (10) Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (The Army Requiring Activity is responsible for providing the contractor with its UIC for the purposes of reporting this information); (11) Locations where contractor and subcontractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website); (12) Presence of deployment or contingency contract language; and (13) Number of contractor and subcontractor employees deployed in theater this reporting period (by country). As part of its submission, the Contractor shall provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period shall be the period of performance not to exceed 12 months ending September 30 of each Government fiscal year and must be reported by 31 October of each calendar year. Contractors may use a direct XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's system to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the website.

15.11 Proprietary Information

In the event that non-COTS, contractor-owned software is used in any task under this task order, the Contractor shall identify these software components to the Government and the Contractor shall grant unlimited use to the Government, in accordance with DFARS 252.227-7013 Rights in Technical Data.

The Government requires unlimited rights to all documents/material and software produced under this Task Order. At a minimum all documents and materials, to include the source codes of any software produced under this task order, shall be provided with Government Purpose Rights. The Government shall have the right to use, modify, reproduce, release, perform, display or disclose technical data or computer software within the Government without restriction or outside the Government for U.S Government purposes. This right does not abrogate any other Government rights. All parties shall use electronic technologies to reduce paper copies of program information generated throughout the life of the task order and to communicate and pass data between government and contractor organizations.

16 **<u>Invoicing.</u>**

The Contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates and quantities of labor hours per labor category.

Note: The Government reserves the right to audit, thus; the Contractor shall keep on file all backup support documentation for Travel, Tools, and ODCs.

16.1 Invoice Requirements.
The Contractor shall submit a draft or advance copy of an invoice to the client POC for review prior to its submission to GSA.

The Contractor shall invoice monthly on the basis of cost incurred for the Labor, Base Fee, Travel, Tools, and ODC CLINs. The Period of Performance (POP) for each invoice shall be for one calendar month. The Contractor shall submit only one invoice per month. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after the end of the invoiced month.

Content of Invoice: The Contractor's invoice shall be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel, tools, and ODCs, ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum:

(a) GSA Task Order Number
(b) Task Order ACT Number
(c) Remittance Address
(d) Period of Performance for Billing Period
(e) Point of Contact and Phone Number
(f) Invoice Amount
(g) Support Items listed by Specific Item and Amount (if applicable) billed to ODC or Tools CLIN as appropriate.
(h) Training Itemized by Individual and Purpose (if applicable) billed to ODC CLIN

All hours and costs shall be reported by CLIN element and contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in a Microsoft Excel spreadsheet format containing separate worksheets showing the information in a format agreed to by the Government. The invoice shall include the period of performance covered by the invoice and the CLIN numbers and titles. The Government reserves the right to modify invoicing requirements at its discretion. The Contractor shall comply with any revised invoicing requirements at no additional cost to the Government.

Interim close-outs: The Government will close out each year of performance within 6 months of its expiration using the rates billed during that period. The contractor will be required to execute a waiver of claims to be included in a bi-lateral modification at the conclusion of the performance period.

Final Invoice: Invoices for the final performance period must be so identified and submitted within 6 months from completion. After this submission, no further charges are to be billed. A copy of the written client agency acceptance of task completion must be attached to the final invoice. If necessary, the contractor may request from GSA an extension for a final invoice that may exceed the 6-month time frame.

After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

The Government reserves the right to require certification by a GSA COR before payment is processed, if necessary.

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance SHALL NOT be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The Contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
Finance Division
P.O. Box 71365
Philadelphia, PA 19176-1365

16.2 Firm-Fixed-Price (FFP) CLINS for LABOR (If applicable)
For FFP Labor CLINs, the Contractor shall invoice in accordance with the payment schedule in PWS Section 11.2 monthly.

16.3 Labor Hour CLINS (If applicable)
For Labor Hour CLINs, the Contractor's invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It shall also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For Labor Hour CLINs each invoice shall clearly indicate both the current invoice monthly "burn rate" and the total average monthly "burn rate".

16.4 TRAVEL *(if allowable and applicable)*
Costs incurred for Travel comparable with the FTR shall be invoiced monthly with travel itemized by Individual and Trip. The Contractor shall provide the Travel invoice data on separate worksheets in Microsoft Excel spreadsheet form with the following detailed information.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel detail shall include separate columns and totals and include the following:

(a) Travel Authorization Request Number or identifier
(b) Current invoice period
(c) Names of persons traveling
(d) Number of travel days
(e) Dates of travel
(f) Location of travel

(g) Number of days per diem charged
(h) Per diem rate used
(i) Total per diem charged
(j) Transportation costs
(k) Total charges

All cost presentations provided by the contractor shall include Overhead Charges and General and Administrative Charges. Fee shall not be permitted on travel costs.

16.5 TOOLS AND ODCs *(if allowable and applicable)*

Costs incurred for the Tools and ODC CLINs shall be invoiced monthly. The Contractor shall provide the Tools invoice data on separate worksheets in Microsoft Excel spreadsheet form with the following detailed information, as applicable:

(a) Tools purchased and/or ODC costs incurred
(b) Consent to Purchase Number or identifier
(c) Description of the Tools with the Quantity, Unit Price and Extended Price of each Tool and/or ODC identified
(d) Date accepted by the Government
(e) Associated CLINs
(f) Project to date totals by CLIN
(g) Cost incurred not billed
(h) Remaining balance of the associated CLINs

All cost presentations provided by the contractor shall also include Overhead Charges, General and Administrative Charges, and or material handling as appropriate and consistent with DCAA recommendations. Feel shall not be permitted on Tools and ODC costs.

16.6 INVOICE SUBMISSION PROCESS:

Invoice submission consists of:

a. Create an Invoice Acceptance Document the GSA Assist portal’s central Invoice Service (CIS), enter the service month, delivery data, invoice number, other pertinent comments and upload requisite backup documentation to obtain Client and GSA Acceptance.
b. Click on the “Submit” button at the bottom of the page to complete the process.

<u>Note:</u> No paper copy of the invoice shall be submitted to GSA unless requested. The Contractor may be required to submit a written “hardcopy” invoice to the Government, or a hardcopy of the invoice with the client’s certification if requested by the GSA COR.

When the Contractor’s acceptance document is submitted, emails requesting Government acceptance are automatically sent to both the Client and the GSA Project Manager/COR. They will accept, partially accept, or reject the invoice, normally with explanatory comments and will indicate the amount approved for payment.

If the Contractor requires assistance or has questions regarding the acceptance and approval process, contact the GSA COR or call the ITSS Help Desk at the toll free number 1-877-243-2889. Be sure to have the ITSS Order number or ACT number available.

To check the payment status of an invoice, go to www.finance.gsa.gov. If you have payment questions, e-mail FW-PaymentSearch.finance@gsa.gov or call the Customer Support Desk at 1-817-978-2408.

17 CLAUSES

FAR 52.252-2 Clauses Incorporated by Reference
The Alliant Small Business contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: http://acquisition.gov/.

52.217-8 Option to Extend Services (NOV 1999)
The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

52.217-9 Option to Extend the Term of the Contract (MAR 2000)
(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

52.216-1 Type of Contract (Apr 1984)
The Government contemplates award of a hybrid Firm Fixed Price/Labor Hour type contract resulting from this solicitation.

52.237-3 Continuity of Services. (JAN 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to—

(1) Furnish phase-in training; and

(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer’s written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer’s approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (*i.e.*, costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

52.249-1 -- Termination for Convenience of the Government (Fixed-Price) (Short Form) (Apr 1984)

GSAM 552.232-78 Payment Information. (Jul 2000)

FAR 52.227-6 -- Royalty Information. (Apr 1984)
FAR 52.227-9 -- Refund of Royalties. (Apr 1984)
FAR 52.227-1 -- Authorization and Consent. (Dec 2007)
FAR 52.227-10 -- Filing of Patent Applications -- Classified Subject Matter. (Dec 2007)
FAR 52.227-11 -- Patent Rights -- Ownership by the Contractor. (May 2014)

FAR 52.227-3 -- Patent Indemnity (Apr 1984)

(a) The Contractor shall indemnify the Government and its officers, agents, and employees against liability, including costs, for infringement of any United States patent (except a patent issued upon an application that is now or may hereafter be withheld from issue pursuant to a Secrecy Order under 35 U.S.C. 181) arising out of the manufacture or delivery of supplies, the performance of services, or the construction, alteration, modification, or repair of real property (hereinafter referred to as “construction work”) under this contract, or out of the use or disposal by or for the account of the Government of such supplies or construction work.

(b) This indemnity shall not apply unless the Contractor shall have been informed as soon as practicable by the Government of the suit or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. Further, this indemnity shall not apply to --

(1) An infringement resulting from compliance with specific written instructions of the Contracting Officer directing a change in the supplies to be delivered or in the materials or equipment to be used, or directing a manner of performance of the contract not normally used by the Contractor;

(2) An infringement resulting from addition to or change in supplies or components furnished or construction work performed that was made subsequent to delivery or performance; or

(3) A claimed infringement that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent jurisdiction.

(c) This patent indemnification shall cover the following items:

This patent indemnification shall be applicable to any patent claims or suits against the Government arising out of any activity occurring pursuant to this task order regarding the making, use or sale of any items, or materials; or the practicing of any processes; which, in either case, have been sold or offered for sale by the contractor or its subcontractors hereunder to the public, in the commercial open market, and to such items, materials, or processes with realtively minor modifications thereto.

(End of Clause)

DFARS 252.227-7039 Patents--Reporting of Subject Inventions. (APR 1990)
DFARS 252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation. (FEB 2014)
DFARS 252.227-7016 Rights in Bid or Proposal Information. (JAN 2011)
DFARS 252.227-7019 Validation of Asserted Restrictions--Computer Software. (SEP 2011)
DFARS 252.227-7013 Rights in Technical Data--Noncommercial Items. (FEB 2014)
DFARS 252.227-7028 Technical Data or Computer Software Previously Delivered to the Government. (JUN 1995)
DFARS 252.227-7030 Technical Data--Withholding of Payment. (MAR 2000)
DFARS 252.227-7037 Validation of Restrictive Markings on Technical Data. (JUN 2013)

Acceptable Skill Level Variation in Severable Labor Hour and Time and Material Orders/Contracts (July/2005)

The contractor may exceed the total number of labor hours per awarded skill level per base or option period, to a limit of 15% as long as the total task order obligated dollar amount per that base or option period is not exceeded, and as long as the contractor maintains an acceptable level of effort throughout the required period of performance. The contractor is not authorized to add new skill level categories or vary between levels within the same labor category without approval of the Government, formalized in a signed modification by the contracting officer.